Department of Justice

United States Attorney Scott W. Brady
Western District of Pennsylvania

FOR IMMEDIATE RELEASE
WEDNESDAY, MAY 8, 2019
WWW.JUSTICE.GOV/USAO/PAW

ADMINISTRATORS OF DEEPDOTWEB INDICTED FOR MONEY LAUNDERING CONSPIRACY RELATING TO KICKBACKS FOR SALES OF FENTANYL, HEROIN, AND OTHER ILLEGAL GOODS ON THE DARKNET

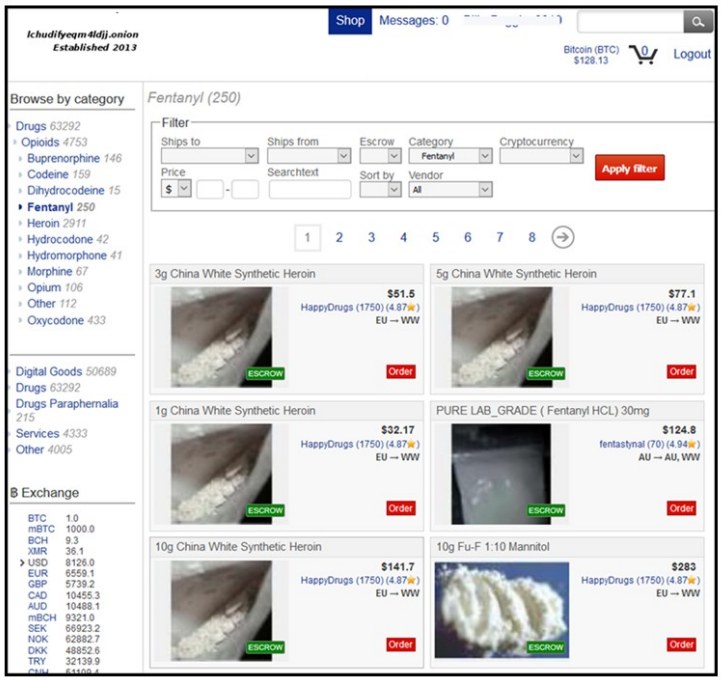
PITTSBURGH - United States Attorney Scott W. Brady announced today the alleged owners and operators of a website known as DeepDotWeb (DDW) have been arrested on charges of money laundering conspiracy relating to millions of dollars in kickbacks they received for purchases of fentanyl, heroin, and other illegal contraband by individuals referred to Darknet marketplaces by DDW. The website has now been seized by court order.

In an indictment unsealed today, Tal Prihar, 37, an Israeli citizen residing in Brazil, and Michael Phan, 34, an Israeli citizen residing in Israel, were charged on April 24, 2019, in a one-count indictment by a federal grand jury in Pittsburgh. Prihar was arrested on May 6, 2019 by French law enforcement authorities in Paris, pursuant to a provisional arrest request by the United States in connection with the indictment. Phan was arrested in Israel on May 6 pursuant to charges in Israel. Further, FBI Pittsburgh seized DDW, pursuant to a court order issued by the U.S. District Court for the Western District of Pennsylvania.

"This is the single most significant law enforcement disruption of the Darknet to date," said U.S. Attorney Scott W. Brady. "With western Pennsylvania at the epicenter of the opioid crisis in America, the U.S attorney's office has leveraged its significant cyber expertise in attacking the sale of fentanyl and opioids on the Darknet. This case signifies the first takedown of the very infrastructure that supports and promotes the illegal marketplaces where these deadly drugs are sold on the Darknet."

According to the indictment, between October 2013 until the date of the indictment, Tal Prihar and his co-conspirator Michael Phan allegedly owned and operated DDW, hosted at www.deepdotweb.com.

DDW provided users with direct access to numerous online Darknet marketplaces, not accessible through traditional search engines, where vendors sold illegal narcotics such as fentanyl, carfentanil, cocaine, heroin, and crystal methamphetamine, firearms, including assault rifles, malicious software and hacking tools stolen financial information and payment cards and numbers access device-making equipment and other illegal contraband.



Prihar and Phan received kickback payments, representing commissions on the proceeds from each purchase of the illegal goods made by individuals referred to a Darknet marketplace from the DDW site. These kickback payments were made in virtual currency, such as bitcoin, and paid into a DDW-controlled bitcoin "wallet." To conceal and disguise the nature and source of the illegal proceeds, totaling over $15 million, Prihar and Phan transferred their illegal kickback payments from their DDW bitcoin wallet to other bitcoin accounts and to bank accounts they controlled in the names of shell companies.

The Money Laundering Kickback Scheme

According to the indictment, Darknet marketplaces operated on the "Tor" network, a computer network designed to facilitate anonymous communication over the Internet. Because of Tor's structure, a user who wanted to visit a particular Darknet marketplace needed to know the site's exact .onion address. DDW simplified this process by including pages of hyperlinks to various Darknet marketplaces' .onion addresses.

How DeepDotWeb Profited by Referring the General Public to Darknet Marketplaces

Users who visited DDW were able to click on the hyperlinks to navigate directly to the Darknet marketplaces. Embedded in these links were unique account identifiers, which enabled the individual marketplaces to pay what they referred to as "Referral Bonuses," to DDW. These kickbacks, paid in virtual currency, were a percentage of the profits of all of the activities conducted on the marketplace by any user who made purchases on the marketplace by using DDW's customized referral link. Through the use of the referral links, DDW received kickbacks from Darknet marketplaces every time a purchaser used DDW to buy illegal narcotics or other illegal goods on the marketplace.

During the time period relevant to this Indictment, DDW's referral links were widely used by users in the Western District of Pennsylvania and elsewhere to access and then create accounts on many Darknet marketplaces, including AlphaBay Market, Agora Market, Abraxas Market, Dream Market, Valhalla Market, Hansa Market, TradeRoute Market, Dr. D's, Wall Street Market, and Tochka Market. These Darknet markets offer illegal drugs, fraudulent identification materials, counterfeit goods, hacking tools, malware, firearms, and toxic chemicals. Two of the largest markets included AlphaBay and Hansa Market, which were both seized by law enforcement in 2017. Approximately 23 percent of all orders completed on AlphaBay and 47% of all orders completed on Hansa were associated with accounts created through DDW referral links, meaning that DDW received referral fees for 23% of all orders made on AlphaBay and 47% of all orders made on Hansa.

During the time period relevant to this Indictment, DDW's referral links were widely used by users in the Western District of Pennsylvania and elsewhere to access and then create accounts on many Darknet marketplaces, including AlphaBay Market, Agora Market, Abraxas Market, Dream Market, Valhalla Market, Hansa Market, TradeRoute Market, Dr. D's, Wall Street Market, and Tochka Market. When AlphaBay was seized by law enforcement in 2017, it was one of the largest Darknet markets that offered illegal drugs, fraudulent identification materials, counterfeit goods, hacking tools, malware, firearms, and toxic chemicals. Approximately 23.6% of all orders completed on AlphaBay were associated with an account created through a DDW referral link, meaning that DDW received a referral fee for 23.6% of all orders made on AlphaBay.

Over the course of the conspiracy, the defendants referred hundreds of thousands of users to Darknet marketplaces. These users in turn completed hundreds of millions' of dollars' worth of transactions, including purchases of illegal narcotics such as fentanyl, carfentanil, cocaine, heroin, and crystal methamphetamine, firearms, including assault rifles, malicious software and hacking tools, stolen financial information and payment cards and numbers, access device-making equipment, and other illegal contraband. Through the use of the referral links, the defendants received kickbacks worth millions of dollars, generated from the illicit sales conducted on Darknet marketplace accounts created through the site.

The defendants grew and promoted the DDW site, which functioned to drive further traffic to the DDW referral links, generating additional income for the defendants. Prihar functioned as the administrator of DDW. He registered the domain, made infrastructure payments and maintained control over site content. Phan was responsible for DDW's technical operations, designing and maintaining the website's day-to-day operation. Phan and Prihar communicated on a daily basis to facilitate their criminal enterprise.

From in or before November 2014 until the date of this indictment, the defendants ,,ontrolled a bitcoin wallet that they used to receive the kickback payments for purchases completed on the various Darknet marketplaces. Throughout the course of the conspiracy, DDW operated accounts on Darknet markets and communicated with the operators of various Darknet markets regarding kickback payments.

Between in and around November 2014 and April 10, 2019, DDW received approximately 8,155 bitcoin in kickback payments from Darknet marketplaces, worth approximately $8,414,173 when adjusted for the trading value of bitcoin at the time of each transaction. The bitcoin was transferred to DDW's bitcoin wallet, controlled by the defendants, in a series of more than 40,000 deposits and was subsequently withdrawn to various destinations both known and unknown to the grand jury through over 2,700 transactions. Due to bitcoin's fluctuating exchange rate, the value of the bitcoin at the time of the withdrawals from the DDW bitcoin wallet equated to approximately $15,489,415. In seeking to conceal their illicit activities and protect their criminal enterprise and the illegal proceeds it generated, the defendants set up numerous shell companies around the world. The defendants used these companies to move their ill-gotten gains and conduct other activity related to DDW. These companies included WwwCom Ltd., M&T Marketing, Imtech, O.T.S.R. Biztech, and Tal Advanced Tech.

"While there have been successful prosecutions of various Darknet marketplaces, this prosecution is the first to attack the infrastructure supporting the Darknet itself," said U.S. Attorney Brady. The website has been seized by the FBI based on a court order obtained in the Western District of Pennsylvania.

"Websites like DeepDotWeb pose global threats that require global partnerships," said FBI Special Agent in Charge Robert Jones. "DDW acted as a gateway to the Darknet, allowing for the purchase and exchange of illicit drugs and other illegal items around the world, and the individuals charged today profited from those nefarious transactions. The efforts of federal and international law enforcement should send the message that we are coming after the operators of these dangerous websites."

An indictment contains only allegations. A defendant is presumed innocent until proven guilty beyond a reasonable doubt in a court of law.

This case was brought in conjunction with the Hi-Tech Organized Crime Unit, Joint Criminal Opioid and Darknet Enforcement (J-CODE) Team. Announced by the U.S. Attorney General in Pittsburgh, Pennsylvania, in January, 2018, J-CODE is a Department of Justice initiative targeting drug trafficking, especially fentanyl and other opioids, on the Darknet. The J-CODE team brings together experienced prosecutors, agents, analysts and professional staff with expertise in drugs, gangs, health care fraud and cyber-based investigations. J-CODE entities, including the FBI, Drug Enforcement Administration, U.S. Postal Inspection Service, U.S. Customs and Border Protection, U.S. Immigration and Customs Enforcement Homeland Security Investigations, Department of Defense, Financial Crimes Enforcement Network and Department of Justice focus on disrupting the sale of drugs via the Darknet and dismantling criminal enterprises that facilitate this trafficking.

Assistant U.S. Attorney Jessica Lieber Smolar of the U.S. Attorney's Office for the Western District of Pennsylvania, Trial Attorney C. Alden Pelker of the Criminal Division's Computer Crime and Intellectual Property Section, and Trial Attorneys Alexander Gottfried and Joseph Wheatley of the Criminal Division's Organized Crime and Gang Section are prosecuting the case. The FBI's Pittsburgh Field Office is investigating the case. The United States Attorney thanks the French authorities, as well as its law enforcement colleagues at the United States Postal Inspection Service, Internal Revenue Service, Brazilian Federal Police Cyber Division, Israeli National Police, Dutch National Police, Europol Darkweb Team, Federal Criminal Police Office of Germany, and law enforcement in the United Kingdom. Significant assistance was also provided by the United States Department of Justice, Criminal Division's Office of International Affairs.

###